Opis Przedmiotu Zamówienia

na świadczenie usług zaufania w zakresie obsługi składania i weryfikacji podpisu elektronicznego

I. Słownik pojęć

Ustawa - Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

eIDAS- Rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające Dyrektywę Parlamentu Europejskiego i Rady UE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (eIDAS) 1999/93/WE.

Certyfikat podpisu elektronicznego – poświadczenie elektroniczne, które przyporządkowuje dane służące do walidacji podpisu elektronicznego do osoby fizycznej i potwierdza co najmniej imię i nazwisko lub pseudonim tej osoby.

Certyfikat kwalifikowany– kwalifikowany certyfikat podpisu elektronicznego w rozumieniu Ustawy.

Podpis elektroniczny - dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego, jako podpis.

Kwalifikowany podpis elektroniczny - zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego.

Mobilny podpis elektroniczny - zaawansowany podpis elektroniczny opierający się na kwalifikowanym certyfikacie podpisu elektronicznego, nie wymagający użycia fizycznych narzędzi do składania podpisu elektronicznego.

Kwalifikowany Dostawca Usług Zaufania - dostawca usług zaufania, który świadczy przynajmniej jedną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru. Podmiot ten nazywany będzie Centrum Certyfikacji.

Usługi zaufania - Usługa elektroniczna obejmująca:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami.

Znakowanie czasem - usługę polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.

Polityka Certyfikacji - szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki bezpieczeństwa tworzenia i stosowania certyfikatów.

Dni robocze – od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy.

II. Przedmiot zamówienia

1. Przedmiotem zamówienia jest świadczenie usług zaufania w zakresie:

    1) wystawiania certyfikatów kwalifikowanych do mobilnych podpisów elektronicznych ważnego przez okres 24 miesięcy;

2) dostawy zestawów do składania podpisu elektronicznego z certyfikatem kwalifikowanym podpisu elektronicznego ważnego przez okres 24 miesięcy;

3) odnawiania certyfikatów kwalifikowanych podpisu elektronicznego ważnego przez okres 24 miesięcy, w tym już posiadających przez Zamawiającego, a tracących ważność podczas trwania umowy, oraz dostarczonych przez Wykonawcę w ramach umowy;

4) dostawy pakietu 10 000 kwalifikowanych elektronicznych znaczników czasu do wykorzystania w okresie trwania umowy;

III. TERMIN REALIZACJI ZAMÓWIENIA

Zamówienie będzie realizowane w okresie 24 miesięcy od daty podpisania umowy albo do wyczerpania maksymalnej kwoty umowy, jeżeli wyczerpanie tejże kwoty nastąpi przed dniem wygaśnięcia umowy.

IV. MINIMALNE WYMAGANIA DOTYCZĄCE REALIZACJI PRZEDMIOTU ZAMÓWIENIA

1. Usługi zaufania w zakresie obsługi składania i weryfikacji podpisu elektronicznego świadczone będą zgodnie z przepisami zawartymi w **Ustawie** i **eIDAS**.
2. Świadczenie usług zaufania, o których mowa w pkt II obejmuje w szczególności:
   1) wydawanie certyfikatów kwalifikowanych dla wskazanych pracowników Zamawiającego,
   2) weryfikację tożsamości w siedzibie Zamawiającego;
   3) zawieszenie certyfikatu kwalifikowanego,
   4) unieważnianie certyfikatów na wniosek Zamawiającego,
   5) publikowanie list zawieszonych i unieważnionych certyfikatów,
   6) świadczenie wsparcia technicznego zgodnie z Polityką Certyfikacji Wykonawcy.
3. Wykonawca będzie wystawiał i odnawiał certyfikaty kwalifikowane pozwalające na składanie kwalifikowanego podpisu elektronicznego na podstawie zlecenia przekazanego przez Zamawiającego drogą mailową.
4. Zamawiający wraz ze zleceniem, o którym mowa w pkt 3) przekaże Wykonawcy niezbędne dane do przeprowadzenia procesu wystawienia certyfikatu kwalifikowanego zgodnie z procedurami i Polityką Certyfikacji Wykonawcy oraz wskaże sposób weryfikacji, tj.
   a) w siedzibie Zamawiającego,
   b) w punkcie wskazanym przez Wykonawcę, znajdującym się na terenie Warszawy,
   c) samodzielnie przez Zamawiającego na podstawie regulaminu zaproponowanego przez Wykonawcę i przy użyciu elementów dostarczanych przez Wykonawcę.

   Przy czym o wyborze sposobu weryfikacji spośród wymienionych w powyżej wskazanych punktach a)-b) zawsze decyduje Zamawiający.
5. Od momentu otrzymania zlecenia od Zamawiającego, Wykonawca w terminie nie dłuższym niż dwóch dni roboczych skontaktuje się z Zamawiającym w celu ustalenia terminu przeprowadzenia czynności weryfikacji tożsamości wskazanych w zleceniu osób oraz sposób jej przeprowadzenia, zgodnie z pkt 4).
6. W przypadku osób wskazanych do weryfikacji tożsamości w siedzibie Zamawiającego Wykonawca w umówionym terminie oraz miejscu przeprowadzi usługę weryfikacji tożsamości.
7. Zamawiający dopuszcza możliwość samodzielnej realizacji czynności weryfikacji tożsamości i wydawania certyfikatów, na podstawie regulaminu zaproponowanego przez Wykonawcę i przy użyciu elementów dostarczanych przez Wykonawcę.
8. Wykonawca nie będzie pobierał od subskrybenta żadnych dodatkowych opłat za przeprowadzenie weryfikacji tożsamości.

9. Wykonawca będzie świadczył usługi zaufania niezbędne dla obsługi wystawionych certyfikatów kwalifikowanych pozwalających na składanie kwalifikowanego podpisu elektronicznego zgodnie z przyjętymi procedurami i Polityką Certyfikacji, a w szczególności:
    1) na wniosek Zamawiającego przekazany przez Zamawiającego drogą mailową Wykonawca zawiesi lub unieważni wskazane certyfikaty kwalifikowane.
    2) opublikuje unieważnione certyfikaty na liście certyfikatów odwołanych.
10. Wykonawca zobowiązuje się do informowania Zamawiającego, z odpowiednim wyprzedzeniem, o istotnych zmianach oprogramowania lub zmianach adresacji serwerów niezbędnych do świadczenia usług zaufania, weryfikacji podpisów elektronicznych, wydawania certyfikatów, lub znakowania czasem w celu zapewnienia nieprzerwanego dostępu do potrzebnych usług.
11. Wykonawca będzie aktualizował niezbędne oprogramowanie w celu niezwłocznego dostosowania go do zmieniających się standardów, przepisów prawa, nowych wersji systemów operacyjnych komputera, JAVA, przeglądarek internetowych, nowych algorytmów, nowych długości kluczy kryptograficznych i zabezpieczenia przed wykrytymi potencjalnymi zagrożeniami bezpieczeństwa oraz błędami.
12. Wykonawca gwarantuje dostarczanie fabrycznie nowych elementów wchodzących w skład zestawu do składania kwalifikowanego podpisu elektronicznego.
13. **Minimalne warunki świadczenia usługi wystawiania certyfikatów kwalifikowanych do mobilnych podpisów elektronicznych.**
    1) Wykonawca będzie wystawiał certyfikaty kwalifikowane do mobilnego podpisu elektronicznego spełniające poniżej wymienione minimalne warunki:
        a) certyfikat kwalifikowany musi być zgodny z Ustawą i eIDAS;
        b) musi spełniać wymagania aktów wykonawczych wydanych do Ustawy;
        c) musi mieć okres ważności 2 lata;
        d) certyfikat kwalifikowany przechowywany przez Wykonawcę zgodnie z eIDAS;
        e) oprogramowanie: umożliwiające zdalne składanie i weryfikację bezpiecznego podpisu elektronicznego;
        f) kwalifikowane znaczniki czasu w ilości min. 200 znaczników na dobę dla pojedynczego certyfikatu;
        g) wykorzystujący algorytm, obowiązujący dla chwili wystawienia, SHA2, lub lepszy.
14. **Warunki świadczenia usługi odnowienia kwalifikowanych certyfikatów podpisu elektronicznego.**
    1) Wykonawca przeprowadzi proces odnowienia certyfikatów kwalifikowanych pozwalających na składanie kwalifikowanego podpisu elektronicznego, kwalifikowalnego mobilnego podpisu elektronicznego oraz migrację/aktywację wskazanych certyfikatów zapisanych na kartach kryptograficznych do formuły podpisu mobilnego, na kolejny okres ważności 2 lat na podstawie zlecenia przekazanego przez Zamawiającego drogą mailową.
    2) Odnowieniu będą podlegały certyfikaty kwalifikowane CenCert.
    3) Odnowienie ważnego certyfikatu kwalifikowanego nie może powodować konieczności ponownej weryfikacji tożsamości pracownika, w szczególności potrzeby osobistego udawania się do punktu weryfikacji tożsamości.
    4) W przypadku konieczności wymiany karty kryptograficznej w celu przeprowadzenia odnowienia certyfikatu, Wykonawca zobowiązany jest dostarczyć nową kartę.

Wykonawca dostarczy kartę kryptograficzną w takim samym formacie jak karta wymieniana, kompatybilną z posiadanymi przez użytkownika czytnikami kart. W procesie odnawiania certyfikatu na nowej karcie weryfikacja tożsamości pracownika nastąpi zgodnie ze wskazanym w zleceniu sposobie.

5) Zapewnienie niezbędnego do przeprowadzenia odnowienia certyfikatu, specjalistycznego oprogramowania komputerowego leży po stronie Wykonawcy.

6) Wykonawca będzie wystawiał certyfikaty spełniające poniżej wymienione minimalne warunki:

   a) certyfikat kwalifikowany zgodny z Ustawą i eIDAS;

   b) spełniający wymagania aktów wykonawczych wydanych do Ustawy z okresem ważności 2 lata;

   c) karta kryptograficzna fizyczna mini lub certyfikat kwalifikowany przechowywany przez Wykonawcę zgodnie z eIDAS;

   d) oprogramowanie: umożliwiające składanie i weryfikację bezpiecznego podpisu elektronicznego za pomocą urządzeń mobilnych;

   e) kwalifikowane znaczniki czasu w ilości min. 200 znaczników na dobę dla pojedynczego certyfikatu;

   f) wykorzystujący algorytm, obowiązujący dla chwili wystawienia, SHA2, lub lepszy.

15. **Warunki dostarczenia zestawów do składania kwalifikowanych podpisów elektronicznych kwalifikowanym certyfikatem podpisu elektronicznego**

    1) Proces wystawienia certyfikatów kwalifikowanych zostanie zrealizowany zgodnie z wymaganiami opisanymi w pkt IV ppkt. 1 – 12.

    2) Zestawy do składania kwalifikowanego podpisu elektronicznego muszą zawierać co najmniej:

       a) Certyfikat kwalifikowany do składania kwalifikowanego podpisu elektronicznego zgodny z wymaganiami wskazanymi w Ustawie:

          - okresie ważności 2 lata;
          - kwalifikowane znaczniki czasu w ilości min. 200 znaczników na dobę dla pojedynczego certyfikatu;
          - wykorzystujący algorytm, obowiązujący dla chwili wystawienia, SHA2, lub lepszy;

       b) Kartę kryptograficzną (mini) zgodną z wymaganiami Ustawy oraz aktów wykonawczych do niej i eIDAS stanowiącą kwalifikowane urządzenie do składania podpisu elektronicznego.

       c) Czytnik kart kryptograficznych (mini) o poniższych parametrach:

          - złącze USB kompatybilne z USB 2.0, 3.0 i nowszymi;
          - niewymagający dodatkowego źródła zasilania (poza portem USB);
          - kompaktowy, o zwartej konstrukcji niewymagającej używania dodatkowych przewodów do podłączenia do standardowego portu USB komputera;
          - estetycznie wykonany, przystosowany do przenoszenia wraz z kartą kryptograficzną mini;
          - obsługujący w pełnym zakresie dostarczone karty kryptograficzne, lub posiadane przez Zamawiającego w przypadku odnawiania certyfikatów z użyciem tych kart;

- kompatybilny z systemami operacyjnymi MS Windows: 10 i 11. Dostępne sterowniki dla systemów z rodziny Linux;
- kompatybilny z oprogramowaniem służącym do składania i weryfikacji podpisów elektronicznych, kwalifikowanych podpisów elektronicznych oraz zarządzania certyfikatami na karcie kryptograficznej, dostarczonym/udostępnionym przez Wykonawcę.

3) Oprogramowanie do składania i weryfikacji podpisów elektronicznych, w tym podpisów elektronicznych weryfikowanych z wykorzystaniem certyfikatów kwalifikowanych oraz obsługi kart kryptograficznych spełniających co najmniej poniższe wymagania:

   a) dostarczone przez Wykonawcę oprogramowanie do weryfikacji podpisów elektronicznych i kwalifikowanych podpisów elektronicznych powinno być bezpłatne w użytkowaniu i ogólnodostępne dla odbiorców dokumentów podpisanych podpisem wystawianym przy użyciu certyfikatów dostarczonych przez Wykonawcę oraz pozwalać na:

      - weryfikację podpisu elektronicznego złożonego przy użyciu certyfikatu kwalifikowanego wystawionego przez jedno z dostępnych w Polsce kwalifikowanych Centrów Certyfikacji;
      - weryfikację znacznika czasu bez względu na dostawcę tej usługi po stronie osoby podpisującej;
      - zgodne z eIDAS, w tym obsługujące algorytm funkcji skrótu SHA2 oraz różne długości kluczy kryptograficznych.

   b) oprogramowanie do składania podpisu elektronicznego powinno co najmniej umożliwiać realizację następujących funkcjonalności:

      - złożenie podpisu elektronicznego;
      - złożenie kontrasygnaty dla podpisanego dokumentu podpisem elektronicznym;
      - obsługę wielopodpisu;
      - znakowania czasem;
      - składanie podpisów elektronicznych wewnętrznych, oraz zewnętrznych w formacie XAdES i podpisów wewnętrznych w formacie PAdES;
      - składanie podpisu elektronicznego wraz z rodzajem zobowiązania „Proof of approval”, oraz bez zobowiązania;
      - podpisywanie zarówno pojedynczych plików jak też wielu plików jednocześnie;
      - podpisywanie dokumentów w formacie plików XML, plików tekstowych, dokumentów PDF, plików pakietu biurowego MS Office/Open Office, archiwów ZIP, plików binarnych;
      - zgodne z eIDAS, w tym obsługujące algorytm funkcji skrótu SHA2.

   c) Oprogramowanie pozwalające na weryfikację podpisów elektronicznych kompatybilne z systemami operacyjnymi komputera, co najmniej: MS Windows: 10, 11 oraz Linux i Mac OS. Oprogramowanie powinno umożliwić weryfikację wszelkich podpisów elektronicznych w tym składanych za pomocą certyfikatów kwalifikowanych wystawionych przez centra certyfikacji zarejestrowane w Polsce. Oprogramowanie służące do weryfikacji podpisów elektronicznych powinno być bezpłatnie udostępnione do pobrania na witrynie internetowej Centrum Certyfikacji, lub w odpowiednim dla danego systemu operacyjnego komputera/urządzenia

mobilnego sklepie. Oprogramowanie powinno być zgodne z aktualnie obowiązującymi przepisami w tym eIDAS.

d) Oprogramowanie pozwalające na składanie podpisów kompatybilne z systemami operacyjnymi komputera, co najmniej: MS Windows 10,11.

e) Oprogramowanie do zarządzana certyfikatami na karcie kryptograficznej, w tym umożliwiające zmianę kodów PIN i PUK, rejestrację certyfikatu w systemie MS Windows, odczytanie informacji o certyfikatach na karcie, oraz przeprowadzenie odnowienia podpisu, kompatybilne, co najmniej z systemami operacyjnymi komputera MS Windows 10,11.

4) Wykonawca będzie odpowiedzialny za zapewnienie niezawodnej pracy zestawów do składania kwalifikowanego podpisu elektronicznego wraz z dostarczonym oprogramowaniem.

5) Instrukcje obsługi dla użytkowników podpisów elektronicznych nieposiadających wiedzy technicznej w języku polskim, a w tym co najmniej instrukcja weryfikacji ważności podpisów oraz odczytu treści dokumentu, instrukcja składania podpisów, wraz z przypadkiem wielopodpisu, kontrasygnaty, znacznika czasu. Instrukcja odnowienia certyfikatu podpisu kwalifikowanego, instrukcja zarządzania certyfikatami na karcie kryptograficznej w tym wgrywanie certyfikatu, zmiana PIN, zmiana PUK, instrukcje używania i konfigurowania dostarczonego oprogramowania. Instrukcje będą udostępnione w postaci plików PDF dostarczonych wraz z zestawami do podpisu lub udostępnionych na ogólnodostępnej stronie internetowej centrum certyfikacji.

16. **Warunki dostawy pakietu 10 000 kwalifikowanych znaczników czasu do wykorzystania w okresie trwania umowy**

1) Wykonawca na podstawie zlecenia przekazanego przez Zamawiającego drogą mailową dostarczy Pakiet Kwalifikowanych znaczników czasu uprawniający do pobrania co najmniej 10 000 znaczników.

2) Okres ważności pakietu nie może być krótszy od okresu obowiązywania zawartej umowy.

3) Znaczniki będą pobierane przez dostarczone oprogramowanie do składania podpisu elektronicznego, gdy tylko zostanie włączona taka funkcja.

4) Wszelkie niezbędne dane konfiguracyjne oraz klucze dostępu do tej usługi zostaną dostarczone Zamawiającemu w sposób uniemożliwiający dostęp do usługi dla osób trzecich.

5) Wykonawca będzie informował Zamawiającego o ilości wykorzystanych oraz dostępnych znaczników w pakiecie na każde żądanie.

17. **Wsparcie techniczne**

1) Wykonawca będzie świadczył usługi wsparcia merytorycznego w zakresie obsługi kwalifikowanego podpisu elektronicznego w godzinach 8.15 – 16.15 w dni robocze.

2) Wykonawca udostępni wszystkim użytkownikom, dla których wystawiono certyfikat kwalifikowany, w ramach powyższego zamówienia, następujące środki komunikacji: infolinię telefoniczną płatną wg. taryfy za połączenia lokalne i międzymiastowe, adres poczty elektronicznej w celu zapewnienia pomocy w przypadku problemów z obsługą podpisów elektronicznych, certyfikatów kwalifikowanych, elementów zestawów do składania podpisu elektronicznego oraz realizacji usług zaufania.

3) Wykonawca zapewni dostarczenie aktualizacji oprogramowania do obsługi podpisu elektronicznego w przypadku konieczności dostosowania go do zmieniających się przepisów prawa lub zmiany standardów technicznych, dostosowania do nowych wydań systemów operacyjnych komputera, usunięcia usterek, udostępnienia nowych wersji, zmian długości kluczy oraz algorytmów. Nowa wersja może być udostępniona za pośrednictwem witryny internetowej Centrum Certyfikacji.

4) Za konsultacje dokonane ustaloną drogą komunikacji Wykonawcy nie przysługuje dodatkowe wynagrodzenie.

18. **Gwarancja**

1) Wykonawca udziela 24-miesięcznej gwarancji na elementy wchodzące w skład zestawu do składania zaawansowanego podpisu elektronicznego.

2) Wykonawca gwarantuje, że dostarczone lub udostępnione oprogramowanie, oraz sterowniki są wolne od złośliwego oprogramowania, nie będą zawierały reklam, oraz ukrytych funkcji szpiegujących i są bezpieczne do używania zgodnego z ich przeznaczeniem.

3) Wszelkie koszty związane z usuwaniem usterek objętych gwarancją ponosi Wykonawca.